Respecting Privacy

A Compliance Review Tool for Manitoba's Information Privacy Laws

A Special Report

Access & Privacy

Prepared by:

Ombudsman Manitoba

October 2003

104-01345/

Ombudsman Manitoba

750 – 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Telephone: (204) 982-9130
Toll Free in Manitoba
1-800-665-0531
Fax: (204) 942-7803
E-mail: ombudsman@ombudsman.mb.ca

500 av. Portage, pièce 750
Winnipeg (MB) R3C 3X1
Téléphone : (204) 982-9130
Sans Frais au Manitoba :
1-800-665-0531
Télécopieur : (204) 942-7803
Courriel : ombudsman@ombudsman.mb.ca

www.ombudsman.mb.ca

LETTER OF TRANSMITTAL

To the Members of the Manitoba Legislature:

It has been more than five years since the Manitoba Legislature passed *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA). One of the principal lessons the Office of the Ombudsman has learned through its compliance oversight experience has been the need for public bodies and health information trustees to approach the management of personal information more systematically and proactively.

This need is underscored virtually on a daily basis as modern information and communication technologies facilitate the expanding collection, use, and disclosure of personal and personal health information.

Results of a recent survey that point to the Manitoba public's belief that their personal privacy has been eroded during the past number of years is a matter of concern, especially considering that Manitoba's access and privacy legislation came into force during this period. Further details concerning this survey are featured at the beginning of this Special Report to the members of the Manitoba Legislature.

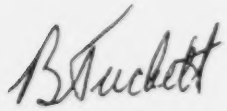
The purpose of this Special Report is to provide a context for and to present a privacy impact assessment process that could significantly enhance both the real and perceived protection of the personal and personal health information of Manitobans. Use of this Privacy Compliance Tool will take resources and commitment, but the payoff will be better privacy protection and increased trust and confidence of the public in how their personal information is being managed.

In some respects, this Special Report is a follow-up to our 1999 report to the Legislature, *A Privacy Snapshot*, which we published

to provide a sense of the privacy environment with the coming into force of FIPPA and PHIA. What we said in the introduction to the Snapshot remains equally valid today:

> *With the accelerating advances in computing and electronic communications, personal information has become a focus of intense interest by many organizations and individuals for a variety of purposes ranging from commerce to research, from service to the public to public safety, and from personal to national security. It has been characterized as a commodity and the protection of it as a human right. While the proper use of personal information can be benign or even beneficial, the abuse of it can lead to consequences ranging from the merely irritating to the terrifying.*

Under section 58(3) of *The Freedom of Information and Protection of Privacy Act* and section 37(3) of *The Personal Health Information Act*, the Provincial Ombudsman may, in the public interest, publish a Special Report relating to any matter within the scope of the powers and duties of the Ombudsman. Among these responsibilities is a duty to inform the public about these two enactments. As well, the Ombudsman's Office serves as an oversight function concerning the collection, use, disclosure and security of personal information and personal health information.



Barry Tuckett
Ombudsman

RESPECTING PRIVACY

A Compliance Review Tool for Manitoba's Information Privacy Laws

Contents

What do Manitobans Think About their Information Privacy? 6

Personal Information Privacy 7

Purpose of this Special Report 7

About FIPPA and PHIA 8

The Privacy Compliance Tool 8

What is Privacy? 9

Privacy and Services to the Public 9

A Backward Glance Before Moving On 10

- *September 11, 2001*
- *Information and Communication Technologies and Better Services*
- *The "Want" or "Need" to Use Personal Identifying Information*

Due Diligence and Risk Management 12

Risks Associated with Not Conducting a Privacy Assessment 12

Using the Privacy Compliance Tool 13

APPENDIX 1: The *Checklist at a Glance* 15

APPENDIX 2: *Principles of Fair Information Practices* 26
(Canadian Standards Association)

What do Manitoban's Think About their Information Privacy?

Six out of every ten Manitobans believe that they have less personal privacy than just five years ago according to survey results released to the Office of the Manitoba Ombudsman by EKOS Research Associates.[1]

In fact, a majority of Manitobans hold the view that "real" personal privacy has become so eroded that it no longer exists in some respects. Specifically, 75% agree that there is "no real privacy" because the government can learn anything it wants about individuals. At least one in two Manitobans (55%) believe that it is more likely than not that they will suffer a serious invasion of privacy during the next two years.

The Manitoba Legislature passed *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA) in June 1997 to protect the public's personal and personal health information. PHIA was proclaimed in December 1997 and FIPPA in May 1998.

EKOS survey results indicate that approximately seven in ten Manitobans are vaguely (26%) or clearly (35%) aware of laws that place strict restrictions on how provincial government departments are able to use or share their personal or personal health information. Nevertheless, Manitobans are cautious in their belief that these laws are being adhered to appropriately. About one in four (26%) report that they are highly confident that the Government will follow its own privacy laws. The remainder have low (19%) to moderate confidence (50%), or did not know or did not respond.

Considering that the provision of personal or personal health information is normally not a matter of choice for people in obtaining essential provincial public services and benefits, we find these figures to be a matter for concern. There should be a higher level of public trust and confidence in how personal and personal health information is handled by entities covered by Manitoba's privacy laws.

It is interesting to view the mandatory requirement for personal information in return for obtaining public services in a context that includes the marketplace, where consumers routinely expect options to be available for acquiring goods and services. In the private sector, no less than two-thirds of Canadians would stop shopping at a favourite store and three in four would consider switching their financial institution if they felt their information were being misused. Such options are not ordinarily available in the public sector.

A particularly disturbing survey finding, considering the implications, was that more than one in ten Manitobans (12%) have withheld personal information from a health care provider because of privacy concerns.

Such results underline a reality that the implications of a privacy breach, or simply the perception of a breach, have deeply significant consequences for individuals, businesses, and government.

1 EKOS Research Associates Inc., "The Rethinking the Information Highway Study", 2002-03 edition.

RESPECTING PRIVACY

A COMPLIANCE REVIEW TOOL FOR MANITOBA'S INFORMATION PRIVACY LAWS

PERSONAL INFORMATION PRIVACY

Information privacy is an important matter of public policy as well as of law, principles, and practices.

Privacy is also a recurring topic of media coverage in North America and abroad. Not a single day goes by without our office receiving literally scores of reports from news services involving privacy issues, developments, concerns, and about breaches of the right to privacy touching people ranging in numbers from one to tens of thousands and more. The stories probably represent but a small proportion of the greater and lesser privacy violations that do not make the news in the course of a year. These reports remind us of the vulnerability and susceptibility of personal information to sometimes well-intentioned but ill-considered collections, uses, and disclosures; to theft and other unlawful practices; and to lax security measures.

While we do not take these news reports as a measure of personal information privacy protection in Manitoba, our experience suggests that it would be prudent, good practice, and in the public interest to ensure that the requirements of Manitoba's privacy legislation are better known, more fully considered, and more systematically applied than is now the case.

PURPOSE OF THIS SPECIAL REPORT

The purpose of this Special Report to the Members of the Manitoba Legislature is to present a privacy impact assessment process that we believe can significantly enhance protection of the public's personal and personal health information privacy under *The Personal Health Information Act* and *The Freedom of Information and Protection of Privacy Act*.

A privacy impact assessment is both a structured due diligence process and a personal information management diagnostic tool to assist organizations in reviewing their compliance with statutory privacy requirements and "best practices". Such an assessment requires a thorough analysis of an organization's policies and activities that have an impact on the information privacy of individuals.

The Privacy Compliance Tool being introduced here has been designed specifically for use under Manitoba's information privacy laws by public bodies and personal health information trustees to pinpoint any area of non-compliance that should be addressed to properly protect the privacy of individuals. It should be used by any entity that is developing or revising a program, a practice, legislation, information system, or embarking on any other initiative that involves identifiable personal or personal health information. It may also be used to review existing programs. A clear intention of Manitoba's legislation is to prevent breaches of information privacy before they occur to the extent possible. As many have said, once privacy is lost, it is lost, and little or nothing can be done to restore it.

Central purposes of FIPPA are to control the manner in which public bodies may collect personal information from individuals and to protect individuals against unauthorized use or disclosure of personal information by public bodies....

Central purposes of PHIA are to control the manner in which trustees may collect personal health information, to protect individuals against the unauthorized use, disclosure or destruction of personal health information by trustees [and]to control the collection, use and disclosure of an individual's PHIN....

A clear intention of Manitoba's legislation is to prevent breaches of information privacy before they occur....

ABOUT FIPPA AND PHIA:

The Freedom of Information and Protection of Privacy Act (FIPPA) and *The Personal Health Information Act* (PHIA) were passed by the Manitoba Legislature in June 1997. PHIA was proclaimed in December 1997 and FIPPA in May 1998. Protecting personal and personal health information privacy is a requirement in Part 3 respectively in each of these Acts.

The Government of Manitoba passed these laws to set out the requirements for managing personal and personal health information held by public bodies and trustees.

The Government of Manitoba passed these laws to set out the requirements for managing personal and personal health information held by public bodies and trustees.[2] The Acts prescribe a number of information management practices regarding the collection, use, disclosure, retention, and security of this information. In these statutes,

- ***personal information*** is recorded information about an identifiable individual including, for example, a person's name, address or home telephone number, age, gender, sexual orientation, marital or family status, religious belief or association, hereditary characteristics, education, employment, criminal history, an identifying number (e.g. case file number, credit card number or social insurance number), and financial and health information.

- ***personal health information*** is recorded information about an identifiable individual that relates to the individual's health, health care history, genetic information, the provision of and payment for health care, and includes the Personal Health Identification Number (PHIN) or other identifying particular assigned to the individual, and any identifying information that is collected in the course of and is incidental to the provision of and payment for health care.

THE PRIVACY COMPLIANCE TOOL

We are pleased to offer a Privacy Compliance Tool (PCT) that focuses on the provisions of FIPPA and of PHIA, the latter being the first of its kind in Canada to deal specifically with personal *health* information. These complementary statutes have a common base of internationally accepted principles of fair information practices. The PCT consists of a Privacy Compliance *Checklist* and a *Guide*. The *Guide* serves to remind users of the statutory requirements and identifies some best practices to assist in completing the *Checklist*. The *Checklist* provides organizations with a step-by-step self-assessment process covering the basic requirements of good information privacy practices.

The Privacy Compliance Tool is intended to fill what we see as a significant gap in the administration of Manitoba's information privacy regime.

The Privacy Compliance Tool is intended to fill what we see as a significant gap in the administration of Manitoba's information privacy regime. At the same time, we are conscious that our office cannot compromise its role as an independent and impartial oversight office by suggesting that its use will eliminate privacy risks and breaches. Nevertheless, it will certainly help organizations comply with the legislation and meet due diligence requirements. We encourage the use of this tool to assess existing programs or before proceeding with new programs, practices, systems, and initiatives that may have an impact on privacy. Additionally, familiarity with the PCT should help increase awareness and understanding of the personal information management rules implicated by FIPPA and PHIA. It will also assist our office in terms of reviewing compliance with the legislation.

2 PHIA encompasses health professionals such as doctors, dentists, physiotherapists, and chiropractors; health care facilities such as hospitals, medical clinics, personal care homes, community health centres, and laboratories; health services agencies that provide health care under an agreement with a trustee; and public bodies as defined under FIPPA. Public bodies include provincial government departments, offices of the ministers of government, the Executive Council Office (Cabinet), and agencies including certain boards, commissions or other bodies; local government bodies such as the City of Winnipeg, municipalities, local government districts, planning districts and conservation districts; educational bodies such as school divisions, universities and colleges; and health care bodies such as hospitals and regional health authorities.

To provide a flavour of the *Guide* and *Checklist*, we have attached a *Checklist at a Glance* as ***Appendix 1***. This document captures the structure of the full *Checklist*, includes all the questions and interrogative statements of the full *Guide* and *Checklist*, but does not provide the detailed explanatory notes, comments, definitions, statutory references or recommended best practices.

WHAT IS PRIVACY?

Privacy is a legal right and many believe that it is a fundamental human right. During the past decade or so, the concern for privacy has taken on increasingly complex dimensions as information networks have expanded our ability exponentially to access information. The particular aspect of privacy that relates to the collection, use, disclosure, storage, and general management of personal information is known as information privacy.

Privacy is a legal right and many believe that it is a fundamental human right.

The concept of information privacy recognizes an individual's right to determine when, how, and to what extent he or she shares personal information with others.

In order to maintain the trust and confidence of clients, employees, patients, and the public, it is essential that government, public bodies and personal health information trustees respect the privacy and security of identifying personal and personal health information.

PRIVACY AND SERVICES TO THE PUBLIC

In recent years, we have noted a growing interest among Manitoba's public bodies and trustees in the development of a privacy compliance assessment tool specific to the Province's access and privacy legislation. Several other jurisdictions have developed privacy impact assessments as a critical methodology to identify privacy concerns and to mitigate risks and harms inherent in the collection, use, disclosure, and retention of personal information in the delivery of goods and services to the public in today's computing and communications environment.

Governments and health care providers deliver a wide range of services to the public. In the course of offering these services, they acquire and have custody or control of extensive and diverse quantities of personal and personal health information. This information often *must* be given by an individual in order to receive the service or benefit. The mandatory nature of such transactions between an individual and the service provider is moderated by the application of fair information practices[3] and information privacy laws passed by the Manitoba Legislature.

Under these principles and laws, the "exchange" of personal and personal health information for services is imbedded in a trust relationship that no more personal information will be collected, used, or disclosed than is necessary for providing a service or as permitted by law; that no one will have access to the information except on a need-to-know basis or as permitted by law; and that the information will retained, protected, and destroyed as permitted or required by law.

Privacy protection should be treated as a normal, routine, and fundamental part of corporate and operational planning.

3 In 1996, the Canadian Standards Association launched a Model Code for the Protection of Personal Information and subsequently adopted it as a "National Standard". This code is reproduced in summary form as Appendix 2 of this Special Report. This code provided much of the infrastructure of the federal government's Personal Information Protection and Electronic Documents Act (PIPEDA), which received Royal Assent in the year 2000. This Act will come into force On January 1, 2004, with respect to the collection, use, and disclosure of personal information in the course of any commercial activity in Manitoba, including provincially regulated organizations in the absence of "substantially similar" provincial legislation.

...the Privacy Compliance Tool is not intended to dislodge any effective instrument that is already in place, but we do invite public bodies and trustees to use it as a measure of or as a supplement to any existing tool.

FIPPA and PHIA were designed to protect personal and personal health information privacy, not to place obstacles in the way of achieving corporate and operational objectives. Privacy protection should be treated as a normal, routine, and fundamental part of corporate and operational planning. Use of this *Checklist* and *Guide* will help management, staff, and contracted agents build information privacy compliance into the everyday business of their organizations.

Some public bodies or personal health information trustees may have a privacy impact assessment template that they have used, but we do not know that this is the case. In any event, the Privacy Compliance Tool is not intended to dislodge any effective instrument that is already in place, but we do invite public bodies and trustees to use it as a measure of or as a supplement to any existing tool.

A BACKWARD GLANCE BEFORE MOVING ON

In 1999, the Manitoba Ombudsman issued his first Special Report to the Legislature by way of introducing the "lay of the land" in information privacy following the proclamation in of PHIA in December 1997 and FIPPA in May 1998.

Addressing the Members of the Manitoba Legislative Assembly through a Special Report entitled, *A Privacy Snapshot taken September 1999*,[4] the Ombudsman wrote:

> *In view of the many recent unprecedented, complex and dynamic privacy issues touching the public, government and our office, this Special Report has been prepared as a "Snapshot" of today's privacy environment.*

As we look back over the more than five years since FIPPA and PHIA came into force, the words of the 19th century French satirist Alphonse Karr come to mind in relation to our first Special Report: "The more things change, the more they stay the same."

September 11, 2001

No other event in recent years than the terrorist attacks in the United States on September 11, 2001, has focussed more clearly the tensions between civil rights and liberties and the needs for public safety and national security.

No other event in recent years than the terrorist attacks in the United States on September 11, 2001, has focussed more clearly the tensions between civil rights and liberties and the needs for public safety and national security. However, attributing the current unstable or – as some would say – embattled state of personal information privacy to these attacks would not recognize that many personal privacy issues had already reached a significant level of national and international exposure.

In the early 1970s, the use of what was then commonly called "automatic data processing" was spreading rapidly through public and private sector organizations. Some of the implications for privacy of this technology were soon realized in North America and Europe. At the same time, the convergence and integration of wired and broadcast communication technologies with data processing capabilities was also well underway, epitomized in some respects by today's Internet, which has moved from a limited to an open network for the transmission of information.

In 1980, the Organisation for Economic Co-operation and Economic Development (OECD) introduced *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, which Canada adopted in 1984. These guidelines established what has become known as the principles of fair information practice that form the core of modern information privacy protection statutes in Canada and elsewhere.

4 Our Special Report to the Legislature, A Privacy Snapshot taken September 1999, provides information and commentary on the general privacy environment to the year 2000 and is available on our web site at: http://www.ombudsman.mb.ca/reports/snapshot.htm

By the year 2000, information and communication technologies in relation to privacy matters had become a multi-faceted subject of vigorous and even bitter international discussion and debate, especially in relation to their actual and potential uses for surveillance purposes. The events of 9/11 intensified rather than introduced the now familiar concerns about finding a reasonable relationship between privacy and public safety or security matters in the use of modern information and communication technologies.

The events of 9/11 intensified rather than introduced the now familiar concerns about finding a reasonable relationship between privacy and public safety or security matters in the use of modern information and communication technologies.

Information and Communication Technologies and Better Services

For the better part of the past three decades, the rapid and accelerating development of information processing and communications technologies have set the pace for a defining social, cultural, political, and economic characteristic of our time: globalization.[5] In this world view, almost everything can be seen as being connected and information knows no border whether geopolitical or technological.

In this world view ["Globalization"], ... almost everything can be seen as being connected and information knows no border whether geopolitical or technological.

Organizations, including governments, have long recognized and responded to a variety of pressures to provide their goods and services more efficiently and effectively. The better use of information has often been touted as the master key to better services. In recent decades, the rapid and pervasive development of Information and Communication Technologies (ICTs) has been described as exerting a compelling "push" for the wider use of the technologies themselves, with applications for business and program purposes providing an intensifying or reinforcing "pull".

There is no doubt that ICTs have already provided important benefits for the provision of public services in – to name but a few – health, education, social assistance, agriculture, the workplace, environment, and law enforcement. Many service providers believe that these achievements are not much more than early explorations or harbingers of future applications of ICTs that will enhance service delivery.

The "Want" or "Need" to Use Personal Identifying Information

In this dynamic situation, where, one way or another, people are at the centre of the reasons for organizations existing, the pressure is intense to use personal identifying information as the essential means of making sense of and using the vast amounts of data available. Even at the current level of development and integration of information processing and communications technologies, it no longer seems farfetched to believe that the time is near when any random bit of recorded or transmitted information about anyone, anywhere could be brought together with other bits and sent anywhere at any time to provide an astonishingly complete picture of that individual in a record or in real time.

...the pressure is intense to use personal identifying information as the essential means of making sense of and using the vast amounts of data available.

The immense volume of personal information already being managed electronically by the health care and public sectors in Canada would, if held in paper form, require literally scores of records warehouses – more likely hundreds. This spatial concentration of information underlines the compelling and urgent need for organizations to be in full command of their personal information collection, use, disclosure, retention and security practices. Otherwise the risks of privacy breaches are significantly magnified over those relating to paper-held records.

[The]... concentration of [electronic] information underlines the compelling and urgent need for organizations to be in full command of their personal information collection, use, disclosure, retention and security practices.

5 This complex and multidimensional concept has been defined by the Canadian Government as describing "the increased mobility of goods, services, labour, technology and capital throughout the world. Although globalization is not a new development, its pace has increased with the advent of new technologies, especially in the area of telecommunications." (See: http://canadianeconomy.gc.ca/english/economy/globalization.html)

Federal and provincial governments everywhere in Canada are already using or implementing or examining ICTs with the avowed purpose of providing better, more economical, and effective services in most areas of their jurisdictions. A particularly notable example is the prospective development of a pan-Canadian Electronic Health Record.[6] The establishment of such a health information network has been the subject of study and recommendations for some years and appears to be on the verge of getting underway in earnest. Expected to cost in the billions of dollars, we could anticipate the development this EHR to be a matter of significant public consultation and discussion in the near future.

The establishment of [a pan-Canadian Electronic Health Record]...has been the subject of study and recommendations for some years and appears to be on the verge of getting underway in earnest.... Public trust and confidence in the information privacy protections underlying such a project will be key enabling factors in making it a success.

Public trust and confidence in the information privacy protections underlying such a project will be key enabling factors in making it a success. Central to the public's view will be assurance that all parties involved in the EHR comply with information privacy laws, principles, and policies relating to the collection, use, disclosure, retention, and security of the personal health information utlilized.

DUE DILIGENCE AND RISK MANAGEMENT

Among other things, a privacy compliance review is an effective due diligence and risk management process requiring direction and commitment from the executive level of organizations.

Among other things, a privacy compliance review is an effective due diligence and risk management process requiring direction and commitment from the executive level of organizations. While the need to undertake a review may be identified at any organizational level, the end product should be to provide the results of the assessment for executive review, sign-off, and decision-making for any actions or direction that may result, thus closing the accountability loop.

Conducting a thorough privacy compliance review in the early stages of developing or modifying a program, practice, system or legislation can help ensure that privacy requirements are identified and satisfied in a timely and cost-effective manner....

This Privacy Compliance Tool may be used as the foundation to assess the information privacy compliance of existing programs. It is especially timely to conduct a review when a new program, practice, information system or legislation is under development or is being modified if that program or system collects, stores, uses, or discloses personal or personal health information. Conducting a thorough privacy compliance review in the early stages of developing or modifying a program, practice, system or legislation can help ensure that privacy requirements are identified and satisfied in a timely and cost-effective manner, that privacy-invasive initiatives are not implemented, that privacy breaches are avoided to the extent possible, and that organizations are not faced with having to undertake expensive revisions or even to cancel a costly initiative after implementation.

RISKS ASSOCIATED WITH NOT CONDUCTING A PRIVACY ASSESSMENT

The general risks associated with failing to undertake a systematic privacy assessment are typically categorized as follows:

- Foremost is the risk for the information privacy of individuals in the knowledge that once privacy has been lost, it usually cannot be fully reinstated.

6 Manitoba was in the forefront of governments in Canada to embark on a major project to establish a Health Information Network. Announced in 1994, it was cancelled in 2000 without having achieved its main objective of suppling health care providers with easier and faster access to a substantial range of vital patient information. The prospective development of a Manitoba Health Information Network was a primary motive behind the province having the distinction of passing the first dedicated personal health information protection statute in the country: The Personal Health Information Act. Notably, the fourth clause of the preamble to the Act reads: "...clear and certain rules for the collection, use and disclosure of personal health information are an essential support for electronic health information systems that can improve both the quality of patient care and the management of health care resources".

- The program or legislative initiative may be brought into discredit with a significant and sometimes even a critical loss of public trust and confidence in an organization's regard for or consideration of the public's legal rights.
- Electronic systems in particular, but also programs, may have to be reconsidered, redesigned, or retro-fitted at substantial cost.
- Personal or personal health information is disclosed or "shared" through existing agreements that may not comply with the legislation or "best practices", or without any written agreement at all.
- Liabilities may ensue for employees and the organization.

USING THE PRIVACY COMPLIANCE TOOL

Undertaking a full privacy compliance review usually requires commitment from the organization involved. For this reason, we reiterate the importance of obtaining senior-level guidance and direction from the outset, bearing in mind that the results should be signed-off by executive decision-makers.

A thorough compliance review may well be an onerous task whose degree of difficulty will be influenced by a number of factors in addition to senior management commitment to fair information practices. These include the privacy expertise available in or to the organization; the extent to which personal and personal health information is collected, used, and disclosed by programs and information systems; the sensitivity of the information involved; the quality, currency, and pervasiveness of effective recordkeeping and information management practices; and the magnitude of the operation or programs involved.

Use of the Checklist will help entities subject to FIPPA and PHIA identify policies, processes, and organizational structures that are not responsive to the requirements of the legislation and to develop plans to bring non-compliant programs, practices, activities, and information systems into conformity with information privacy requirements.

Use of the Checklist will help entities ... bring non-compliant programs, practices, activities, and information systems into conformity with information privacy requirements.

The Checklist contains the considerations for assessing compliance and may be used by the Ombudsman's Office as a guideline for privacy audits or investigations. Using a privacy impact assessment process will help minimize information privacy breaches, but it may not entirely remove risk even when the overall scheme of a program or legislative proposal appears to comply with statutory requirements. Specific breaches will, unfortunately, occur from time-to-time and will have to be dealt with on a case-by-case basis. Nevertheless, a resulting compliance review or investigation by the Ombudsman will take account of the degree of due diligence having been practised through the employment of a privacy impact assessment.

Appendix 1

PRIVACY COMPLIANCE TOOL

CHECKLIST AT A GLANCE

INTRODUCTION

The purpose of this summary form of the larger *Checklist* is to provide users with a quick overview of the questions included in the privacy assessment. This document will facilitate keeping a record of answers and assessing overall compliance.

TABLE OF CONTENTS

ELEMENT 1: Identifying Purposes and Limiting Collection of Personal Information and Personal Health Information 16

ELEMENT 2: Limiting Use, Disclosure and Retention of Personal Information and Personal Health Information 17

ELEMENT 3: Ensuring Accuracy of Personal Information and Personal Health Information 20

ELEMENT 4: Safeguarding Personal Information and Personal Health Information 21

ELEMENT 5: Ensuring Individual Access to Personal Information and Personal Health Information 23

ELEMENT 6: Challenging Compliance 23

ELEMENT 7: Accountability and Openness of Policies and Practices 24

ELEMENT 8: Assessing Privacy Risks in Electronic Service Delivery 25

ELEMENT 1

Identifying Purposes and Limiting Collection of Personal Information and Personal Health Information

\# Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There is a detailed description of the type of *personal information*, *personal health information*, or personal data elements collected for this program or initiative.						
2. The purpose for collecting this *personal information* is authorized according to FIPPA. It is one of the following:† a. authorized by an enactment of Manitoba or Canada, or b. directly related to and is necessary for a program or activity of the *public body*, or c. necessary for law enforcement or crime prevention.						
3. *Personal health information* is not collected unless it is: a. for a lawful purpose connected with a function or activities of the *trustee*; and, b. is necessary for that purpose.						
4. *Personal information* or *personal health information* is collected only directly from the subject individual or his or her authorized representative.						
5. If *personal information* or *personal health information* is collected indirectly (i.e. from a third party), the *indirect collection* is authorized under Section 37(1) of FIPPA or Section 14 of PHIA.						
6. Individuals are informed (notified) of the purpose, authority (where FIPPA is involved) for *collection*, and how to contact an officer or employee who can answer their questions about *collection*.						

† NB: Please specify whether (a), (b), or (c) applies. If it is (a), identify the enactment(s) and applicable section(s).

1 Attachments offer additional information on what exists (e.g. a security policy) whereas Action Plans provide details on corrective or developmental actions that need to be taken (e.g. develop a training program to provide privacy and security awareness for staff).

ELEMENT 2

LIMITING USE, DISCLOSURE AND RETENTION OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

 # LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
A. Limiting Use						
1. *Personal* or *personal health information* is used only for the purpose for which it was obtained or for a use consistent with that purpose under FIPPA or directly related to that purpose under PHIA.						
2. *Consent* is obtained from the individual before using *personal information* for a purpose NOT consistent with the purpose for which it was collected or, in the case of *personal health information*, for a purpose NOT directly related to the purpose for which it was collected.						
3. There is a list of the staff position or categories that *use* this collection of *personal* or *personal health information*.						
4. Physical, administrative, and technical controls limit access to identifiable *personal* and *personal health information* to those who have a "need to know".						
5. The least amount of *personal information* and *personal health information* is used to meet the stated purpose.						
6. *Personal* or *personal health information* is used with the highest degree of *anonymity* to meet the stated purpose.						
B. Limiting Disclosure						
1. Individual consent is obtained before disclosing *personal* or *personal health information* to another government department or agency, *local public body*, *trustee* or other third party.						
2. If *consent* is not obtained, the *disclosure* is authorized according to a specific provision of Section 44(1) of FIPPA or Section 22(2) of PHIA.						
3. When *disclosure* is required and authorized, the amount and type of information disclosed is limited on a "need to know" basis.						
4. *Disclosure* is made at the highest degree of *anonymity* possible while still meeting the purpose of the recipient.						
5. Staff maintains a *disclosure* log or audit trail of:						
a. what information has been disclosed,						
b. to whom it has been disclosed, and						
c. the purpose and authority for the *disclosure*.						

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N	Y	N

C. Uses and Disclosures of Personal Information Not Otherwise Authorized under Division 3 of FIPPA

1. **For a *public body*** other than a *local public body* under Section 46 of FIPPA:
   The proposal or request has been referred to the Privacy Assessment Review Committee (PARC) for its advice:

   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for *disclosure* on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information.*

2. **For a *local public body*** under Section 46 of FIPPA:
   The proposal or request has been either assessed internally by the *local public body* or referred to the Privacy Assessment Review Committee (PARC) for its advice:

   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for *disclosure* on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information.*

3. For the *uses* or *disclosures* contemplated under Section 46 of FIPPA, the Head of the *Public Body* or *Local Public Body* has considered advice received through the statutory privacy assessment review process and approved conditions that must be met under Section 46(6), including a written agreement with the recipient of the *personal information.*

D. Disclosure of Personal Information for a Research Purpose under FIPPA

1. The Head of the *Public Body* or *Local Public Body* has considered any privacy assessment advice requested under Section 47(2) of FIPPA and approved conditions that must be met under Section 47(4), including a written agreement with the recipient of the *personal information.*

 # LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
E. Disclosure of Personal Health Information for a Research Purpose under PHIA						
1. The *personal health information* required for the health research project is recorded information about an identifiable individual that relates to:						
a. the individual's health, health history (including genetic information about the individual), or						
b. the provision of health care to the individual, or						
c. the payment of health care provided to the individual, *and includes*						
d. the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and						
e. any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care.						
2. The health research project has been approved according to the requirements of PHIA Section 24 by:						
a. the Health Information Privacy Committee (HIPC) if the *personal health information* is maintained by the government or a government agency, or						
b. an institutional research review committee if the *personal health information* is maintained by a *trustee* other than the government or a government agency.						
3. The researcher and the *trustee* have entered into an agreement under PHIA Section 24(4), and any regulations, in which the researcher agrees:						
a. not to publish the *personal health information* in an identifying form,						
b. to use the *personal health information* only for the purposes of the approved research project,						
c. to ensure that reasonable safeguards are in place to protect the security and *confidentiality* of the *personal health information*, and						
d. to ensure that the information will be destroyed or deidentified at the earliest opportunity consistent with the purposes of the project.						
F. Limiting Retention:						
1. There is a written records/data retention policy that meets all relevant legislative requirements.						
2. *Personal information* and *personal health information* used to make a decision that directly affects an individual are retained for a reasonable period of time to allow the individual to obtain access to it.						

ELEMENT 3

Ensuring Accuracy of Personal Information and Personal Health Information

Legend: "Y" = Yes; "N" = No; "Expl?" = Explanation?; "A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There are procedures in place to verify *personal* or *personal health information* and to manage requests for corrections that comply with FIPPA Sections 38 and 39 or with PHIA Sections 16 and 12.						
2. The authority to modify or correct *personal* or *personal health information* is clearly established to ensure that those without this authority may not or are unable to alter these records.						
3. An audit trail is maintained to document when and by whom a file or record was compiled or updated.						

ELEMENT 4

Safeguarding Personal Information and Personal Health Information

 # Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. Security measures are in place for *personal* and *personal health information* regardless of media format (i.e. paper, photographic, electronic, etc.).						
2. Written information security policies include a definition of roles and responsibilities, and sanctions for breaches of policy.						
3. Staff receives ongoing training about security policies and procedures, and is made aware of the importance of security and *confidentiality* on an ongoing basis.						
4. Security breaches and violations are documented and responded to according to established processes.						
5. Access to *personal* or *personal health information* is regularly monitored and audited.						
6. *Personal* and *personal health information* are stored or maintained in a physically secure location.						
7. *Personal* and *personal health information* in all media are disposed of securely to prevent unauthorized access.						
8. Physical removal of *personal* and *personal health information* of any medium from a secure designated area is always undertaken in a manner and in accordance with procedures that continue to ensure the security of the information at all times.						

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

ELECTRONIC SYSTEMS SECURITY:			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. Users are assigned unique user identifications and passwords for access to *personal* and *personal health information*, and passwords are changed regularly.						
2. Network and application security status is assigned on a "need to know" basis according to the particular requirements of specific roles within the organization.						
3. Access privileges are revoked promptly when required (e.g. when an employee leaves or moves).						
4. Systems contain audit trails for tracking data access, and audit logs provide information about abnormal or unusual access.						
5. Access logs and audit trails are reviewed on a regular basis.						
6. *Personal* and *personal health information* is transmitted by secure means to minimize opportunities for unauthorized or accidental interception by third parties.						
7 Virus protection is implemented and an effective firewall is in place where necessary, for all information systems that contain *personal* or *personal health information.*						
8. External providers of information management or technology services are covered by written agreements dealing with risks including unauthorized access, *use, disclosure*, retention, and destruction or alteration as required under FIPPA Section 44(2) and PHIA Section 25(3).						

ELEMENT 5

Ensuring Individual Access to Personal Information and Personal Health Information

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. A process to respond to access requests under the Act(s) is in place.						
2. Individuals are informed that the organization holds *personal* or *personal health information* about them and that access to that data is provided, except in limited circumstances as defined in legislation.						
3. Requests for access are responded to within the legal time limits at minimal or no cost, or in compliance with legislation.						
4. The requested information is provided in an understandable format and the organization is prepared to explain any terms or abbreviations.						
5. A refusal to grant access to all or part of an individual's information includes clear reasons for the refusal.						

ELEMENT 6

Challenging Compliance

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There are communication policies and procedures in place that ensure individuals are routinely informed that they may make a complaint to the organization and are informed about their statutory right to make a complaint to the Manitoba Ombudsman respecting their *personal* and *personal health information* rights.						

ELEMENT 7

Accountability and Openess of Policies and Practices

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. It is understood and known in the organization that the Head of a provincial government department or agency, or the Head of a *local public body*, or a *trustee* is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded.						
2. An employee (or employees) within the organization is formally delegated responsibility for the daily administration of privacy compliance ("access and Privacy coordinators" under FIPPA, "privacy officer" under PHIA). The identity of the individual(s) is known throughout the organization.						
3. There are written organizational policies and procedures that define the responsibility for protecting *personal* and *personal health information*.						
4. Appropriate staff is provided with on-going training to implement privacy policies and procedures.						
5. Other parties, such as information managers and agents, who may have authorized access to *personal information* or *personal health information* under Parts 3 of FIPPA and PHIA are aware of, and comply with, organizational privacy policies and relevant procedures.						
6. Individuals can obtain information about privacy policies and procedures with reasonable ease.						
7. Under FIPPA, *Personal Information Banks* have been identified, described, are up-to-date, and publicly available as required. [Note that PHIA does not have a corresponding provision in relation to production of a directory including a description of personal information banks.]						
8. Under FIPPA and in the case of a public body that is not a local public body, (1) a record is kept of uses and disclosures not included in the publicly available "Access and Privacy Directory", (2) this record is attached or linked to the personal information involved, and (3) a process is in place to have this information included in the "Access and Privacy Directory". [Note that PHIA does not have a directly corresponding provision.]						
9. A procedure exists for responding to questions or concerns about privacy practices.						

ELEMENT 8[8]

Assessing Privacy Risks in Electronic Service Delivery (ESD)

 # Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. Are diagrams available to illustrate the flow of *personal* and *personal health information* for this project?						
2. Has responsibility for control and custody for all *personal* or *personal health information* processed by the ESD system been identified and assigned?						
3. If the ESD system will process transactions for more than one program, agency or department, have constraints been placed on data integration?						
4. If this ESD project involves the use of common identifiers or a common identification infrastructure, have privacy-enhancing measures been considered to limit risk to privacy?						
5. Will this ESD initiative require *data linking* (data profiling) or *data matching*?						
6. Is there a means of obtaining, authenticating, registering and maintaining individual *consent* electronically, where required?						
7. Have privacy-enhancing technologies and/or techniques been considered for this ESD project?						
8. Have all risks to privacy for this ESD initiative been identified and documented?						
9. Have all risks to privacy for this ESD project been minimized or averted?						
10. Has a comprehensive risk analysis been undertaken to identify and implement appropriate ongoing monitoring and regular auditing requirements to protect *personal* and *personal health information*, including that of end-users, for all aspects of the ESD system?						
11. Have key stakeholders been consulted about the privacy implications of this project?						
12. Where risks to privacy are not completely mitigated, is there a strategy for responding to public concerns over privacy protection?						
13. Have constraints been placed on ESD service providers regarding the *collection, use* and *disclosure* of information subject to FIPPA and PHIA?						
14. Do all contracts related to the implementation of this ESD project contain data protection provisions?						

8 Users are asked to provide **Explanations and/or Action Plans** for ALL questions contained in this Element, regardless of a "yes" or no" response. **Attachments** offer additional information on what exists (e.g. a security policy) whereas **Action Plans** provide details on corrective or developmental actions that need to be taken (e.g. develop a training program and provide privacy and security training for staff).

Appendix 2

PRINCIPLES OF FAIR INFORMATION PRACTICES

CANADIAN STANDARDS ASSOCIATION PRINCIPLES IN SUMMARY MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION (1996)

1. ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. IDENTIFYING PURPOSES

The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by lawful means.

5. LIMITED USE, DISCLOSURE AND RETENTION

Personal information shall not be used or disclosed for purposes other that those which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

La protection de la vie privée

Un outil de révision en respect des lois sur la protection des renseignements personnels au Manitoba

Rapport spécial

Acès à l'information et protection de la vie privée

Préparé par :

Ombudsman Manitoba

Octobre 2003

Ombudsman Manitoba

750 – 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Telephone: (204) 982-9130
Toll Free in Manitoba
1-800-665-0531
Fax: (204) 942-7803
E-mail: ombudsman@ombudsman.mb.ca

500 av. Portage, pièce 750
Winnipeg (MB) R3C 3X1
Téléphone : (204) 982-9130
Sans Frais au Manitoba :
1-800-665-0531
Télécopieur : (204) 942-7803
Courriel : ombudsman@ombudsman.mb.ca

www.ombudsman.mb.ca

LETTRE D'ACCOMPAGNEMENT

Destinataires : Les députés de l'Assemblée législative

Il y a plus de cinq ans que les députés de l'Assemblée législative du Manitoba ont adopté la *Loi sur les renseignements médicaux personnels* (LRMP) et la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP). Une des principales leçons apprises par le biais de son expérience d'omission d'observance est la nécessité pour les organismes publics et les dépositaires de renseignements médicaux d'approcher la gestion de renseignements personnels d'une manière plus systématique et proactive.

Cette nécessité est soulignée presque quotidiennement au fur et à mesure que la technologie moderne de communication et d'information rend l'expansion de la collecte, l'utilisation et la divulgation de renseignements médicaux personnels, plus facile.

Les résultats d'un récent sondage qui démontrent que les Manitobains croient que la protection de leur vie privée s'est érodée au cours des dernières années sont préoccupants, particulièrement puisque la législation sur l'accès et la protection de la vie privée a été promulguée au cours de cette pé-riode. De plus amples détails au sujet de ce sondage sont discutés au début de ce Rapport spécial aux députés de l'Assemblée législative du Manitoba.

L'objectif de ce Rapport spécial est de fournir le contexte à un processus d'évaluation d'impact et d'en présenter le mécanisme qui pourrait améliorer de manière importante et la véritable protection, et la protection perçue, des renseignements personnels et des renseignements personnels médicaux des Manitobains. L'utilisation de cet outil de vérification de la protection des renseignements personnels demandera des ressources et un engagement. Le résultat en sera, toutefois, une protection des renseignements personnels améliorée et une augmentation de la confiance du public dans la méthode de gestion de leurs renseignements personnels.

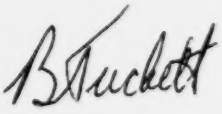
En un sens, ce Rapport spécial est un suivi de notre rapport à l'Assemblée législative de 1999, *Arrêt sur image*, que nous avons

publié afin de fournir un aperçu de l'environnement de la protection de la vie privée suite à la promulgation de la LRMP et de la LAIPVP. Ce que nous avons énoncé dans l'introduction au rapport *Arrêt sur image* demeure également valide aujourd'hui :

> *Les progrès toujours plus rapides qui caractérisent les domaines de l'informatique et des communications électroniques ont suscité l'intérêt de bien des entreprises et des gens pour les renseignements personnels, qui peuvent être utilisés à des fins commerciales ou de recherche, pour fournir des services à la population, ou encore pour assurer la protection de la population et la sécurité nationale. On les considère comme un produit, mais leur protection est perçue comme un droit. Si l'utilisation licite des renseignements personnels est considérée comme inoffensive et même bénéfique, la mauvaise utilisation de ces renseignements peut avoir des conséquences au mieux fâchantes et au pire terrifiantes.*

En vertu du paragraphe 58(3) de la *Loi sur l'accès à l'information et la protection de la vie privée* et du paragraphe 37(3) de la *Loi sur les renseignements médicaux personnels*, l'ombudsman provincial peut, dans l'intérêt public, publier un rapport spécial ayant trait à une question relevant de ses attributions. Le devoir d'informer le public quant à l'existence de ces deux textes législatifs fait partie de responsabilités. L'ombudsman a également un rôle de surveillance quant à la collecte, à l'utilisation, à la divulgation et à la sécurité des renseignements personnels et des renseignements médicaux personnels.

L'ombudsman provincial,



Barry Tuckett

LA PROTECTION DE LA VIE PRIVÉE

UN OUTIL DE RÉVISION EN RESPECT DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AU MANITOBA

TABLE DES MATIÈRES

QUE PENSENT LES MANITOBAINS DE LA PROTECTION DE LEURS RENSEIGNEMENTS PERSONNELS? 6

LA PROTECTION DE RENSEIGNEMENTS PERSONNELS 7

OBJET DE CE RAPPORT SPÉCIAL 7

AU SUJET DE LA LAIPVP ET DE LA LRMP 8

L'OUTIL DE VÉRIFICATION DE LA PROTECTION DE RENSEIGNEMENTS PERSONNELS 8

QU'EST-CE QUE LA PROTECTION DE LA VIE PRIVÉE? 9

LA PROTECTION DE RENSEIGNEMENTS PERSONNELS ET LE SERVICE AU PUBLIC 9

UN REGARD SUR LE PASSÉ AVANT DE CONTINUER 10

- *Le 11 septembre 2001*
- *Les technologies d'information et de communication et de meilleurs services*
- *La « volonté » ou la « nécessité d'utiliser les renseignements d'identification personnels*

LA DILIGENCE RAISONNABLE ET LA GESTION DU RISQUE 12

LES RISQUES ASSOCIÉS AU DÉFAUT D'EXÉCUTER UNE VÉRIFICATION DU RESPECT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 12

L'UTILISATION DE L'OUTIL DE VÉRIFICATION DU RESPECT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 13

ANNEXE 1: *LA LISTE DE CONTRÔLE EN UN CLIN D'OEIL* 15

ANNEXE 2: *LES PRINCIPES ÉNONCÉS DANS LA NORME NATIONALE DU CANADA INTITULÉE CODE TYPE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS* 26

QUE PENSENT LES MANITOBAINS DE LA PROTECTION DE LEURS RENSEIGNEMENTS PERSONNELS ?

Les résultats du sondage de la maison EKOS *Research Associates*[1], fournis au Bureau de l'Ombudsman du Manitoba, démontrent que six Manitobains sur dix croient que leurs renseignements personnels sont moins protégés qu'il n'y a que cinq ans.

En fait, une majorité de Manitobains pensent que la « vraie » protection des renseignements personnels est devenue si minée, qu'elle n'existe plus dans certains secteurs. Précisément, 75 % sont d'accord qu'il n'y a « pas de protection réelle de la vie privée », parce que le gouvernement peut connaître tout ce qu'il désire au sujet des individus. Au moins un Manitobain sur deux (55 %) croit qu'il est probable qu'il fera l'objet d'une invasion sérieuse de ses renseignements personnels au cours des deux prochaines années.

Les députés de l'Assemblée législative du Manitoba ont adopté la *Loi sur les renseignements médicaux personnels* (LRMP) et la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), en juin 1997 afin de protéger les renseignements personnels et les renseignements médicaux personnels du public. La LRMP a été promulguée en décembre 1997, et la LAIPVP en mai 1998.

Le sondage EKOS démontre qu'environ sept Manitobains sur dix sont vaguement (26 %) ou clairement (35 %) informés des lois qui placent des restrictions sévères sur la façon dont les services gouvernementaux provinciaux peuvent utiliser ou partager leurs renseignements personnels ou médicaux. Néanmoins, les Manitobains sont prudents lorsqu'il s'agit de croire que ces lois sont adéquatement respectées. Environ une personne sur quatre (26 %) dit qu'elle a toute confiance que le gouvernement respectera ses propres lois sur la protection de la vie privée. Le reste des gens ont peu confiance (19 %), ou une confiance mitigée (50 %), ne savent pas, ou n'ont pas répondu.

Considérant que la provision de renseignements personnels et médicaux n'est normalement pas une question de choix pour les personnes qui obtiennent des services et des avantages publics provinciaux essentiels, nous trouvons que ces chiffres sont matière à réflexion. Il devrait y avoir un plus haut niveau de confiance publique dans la manière dont les renseignements personnels et médicaux sont traités par les organismes qui tombent sous les lois manitobaines sur la protection de la vie privée.

Il est intéressant de noter la perception de l'exigence obligatoire de renseignements personnels afin d'obtenir des services publics dans un contexte qui comprend la place de marché, où les consommateurs s'attendent, de façon routinière, que des choix seront possibles pour obtenir des biens et services. Dans le secteur privé, pas moins des deux tiers des Canadiens cesseraient de fréquenter un magasin préféré, et trois sur quatre considéreraient changer d'institution financière, s'ils sentaient que leurs renseignements personnels étaient utilisés à mauvais escient. De telles options ne sont généralement pas offertes dans le secteur public.

Un résultat de sondage particulièrement troublant, si on en considère les conséquences, est que plus d'un Manitobain sur dix (12 %) a caché des renseignements personnels des fournisseurs de soins de santé à cause d'inquiétude au sujet de la protection de ces renseignements.

De tels résultats soulignent la réalité que les résultats d'une violation de la protection de la vie privée, ou de la simple perception de la violation, ont des conséquences extrêmement importantes pour les personnes, les établissements d'affaires et le gouvernement.

[1] *EKOS Research Associates Inc., "The Rethinking the Information Highway Study"*. Éd.2002-2003

LA PROTECTION DE LA VIE PRIVÉE

UN OUTIL DE RÉVISION EN RESPECT DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AU MANITOBA

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels est une matière importante de politique publique, tout comme de droit, de principes et de pratiques.

La protection de la vie privée est aussi un sujet récurrent de la couverture médiatique nord-américaine et outremer. Il ne se passe pas une journée sans que notre Bureau reçoive littéralement des vingtaines de rapports de services de nouvelles, au sujet de questions, de développements, d'inquiétudes en ce qui a trait à la protection de la vie privée, et au sujet de la violation du droit à la protection de la vie privée touchant des personnes, en nombre d'une à des dizaines de milliers, et plus. Les articles ne représentent probablement qu'une petite partie des violations petites et grandes qui ne sont pas publiées, au cours d'une année. Ces rapports nous rappellent la vulnérabilité et la sensibilité des renseignements personnels à des collectes, des utilisations et des divulgations quelques fois bien intentionnées, mais non réfléchies; au vol et autres pratiques illégales; ainsi qu'aux mesures de sécurité négligentes.

Alors que nous n'interprétons pas ces rapports à titre de mesure de la protection des renseignements personnels au Manitoba, notre expérience nous suggère qu'il serait prudent, de bonne pratique et dans l'intérêt public de s'assurer que les exigences de la législation manitobaine sur la protection de la vie privée soient mieux connues, examinées plus en profondeur, et appliquées de façon plus systématique, qu'on ne le fait maintenant.

OBJET DE CE RAPPORT SPÉCIAL

L'objet de ce rapport spécial aux députés de l'Assemblée législative est de présenter un processus d'évaluation d'impact de la protection de la vie privée qui, nous croyons, peut améliorer de façon importante la protection des renseignements personnels et médicaux du public, en vertu des *dispositions de la Loi sur les renseignements médicaux personnels et la Loi sur l'accès à l'information et la protection de la vie privée.*

Une évaluation d'impact de la protection de la vie privée est à la fois un processus structuré de diligence raisonnable et un outil diagnostique de gestion des renseignements personnels, afin d'aider les organismes à réviser leur respect des exigences statutaires de la protection de la vie privée et les « meilleures pratiques ». Une telle évaluation demande une analyse en profondeur des politiques et des activités de l'organisme qui ont un effet sur la protection des renseignements personnels des individus.

L'outil de respect de la protection des renseignements personnels présenté ici, a été développé précisément pour être utilisé, en vertu des lois sur la protection des renseignements personnels du Manitoba, par les organismes publics et les dépositaires de renseignements médicaux personnels, afin d'identifier exactement tout aspect de non-respect qui doit être corrigé pour protéger adéquatement le droit à la vie privée de toutes les personnes. Cet outil devrait être utilisé par tout organisme qui développe ou révise un programme, une pratique, une législation, un réseau d'information, ou qui entreprend toute autre initiative qui porte sur les renseignements médicaux

Les objectifs principaux de la LAIPVP est de contrôler la manière par laquelle les organismes publics peuvent collecter les renseignements personnels des individus et de protéger les personnes contre l'utilisation et la divulgation non autorisée de renseignements personnels par les organismes.

Les objectifs principaux de la LRMP sont de contrôler la manière par laquelle les dépositaires peuvent collecter des renseignements médicaux personnels, de protéger les personnes contre l'utilisation, la divulgation ou la destruction non autorisée de renseignements médicaux personnels par les dépositaires (et) de contrôler la collecte, l'utilisation et la divulgation du NIMP d'une personne...

Une intention clair de la législation manitobaine est de prévenir les violations de la protection de la vie privée, avant qu'elles ne surviennent...

personnels identifiables. On peut aussi s'en servir afin de réviser les programmes existants. Une intention claire de la législation manitobaine est de prévenir, dans la mesure du possible, les violations de la protection des renseignements personnels avant qu'elles ne surviennent. Comme on l'a dit souvent, une fois que la protection de la vie privée est perdue, elle est perdue, et on ne peut rien, ou très peu faire, pour la recouvrer.

AU SUJET DE LA LAIPVP ET DE LA LRMP

La Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) et la *Loi sur les renseignements médicaux personnels* (LRMP) ont été adoptées par l'Assemblée législative du Manitoba en juin 1997. La LRMP a été proclamée en décembre 1997 et la LAIPVP l'a été en mai 1998. La protection des renseignements personnels et médicaux est une exigence de la Partie 3 de chacune de ces lois, respectivement.

Le gouvernement du Manitoba a adopté ces lois afin d'établir les exigences pour la gestion des renseignements personnels et médicaux détenus par les organismes publics et les dépositaires.

Le gouvernement du Manitoba a adopté ces lois afin d'établir les exigences pour la gestion des renseignements personnels et médicaux détenus par les organismes publics et les dépositaires[2]. Les lois établissent un nombre de pratiques de gestion des renseignements en ce qui a trait à la collecte, à l'utilisation, à la divulgation, à la rétention et à la sécurité de ces renseignements. Dans ces règlements :

- **Les renseignements personnels** sont les renseignements enregistrés au sujet d'une personne identifiable, y compris à titre d'exemple, le nom d'une personne, son adresse ou son numéro de téléphone à domicile, son âge, son sexe, son orientation sexuelle, son état marital ou familial, ses croyances ou associations religieuses, ses caractéristiques héréditaires, son niveau d'éducation, son emploi, son dossier criminel, un numéro d'identification (p. ex. : numéro de dossier, numéro de carte de crédit ou numéro d'assurance sociale), ainsi que des renseignements financiers ou médicaux.

- **Les renseignements médicaux personnels** sont les renseignements enregistrés au sujet d'une personne identifiable qui se rapportent à la santé de cette personne, son historique de soins de santé, ses renseignements génétiques, les fournitures et le paiement de soins de santé et comprennent le numéro d'identification médicale personnel (NIMP) ou d'autres éléments d'identification précis assignés à la personne, ainsi que tout renseignement d'identification qui est collecté au cours de la fourniture ou au paiement de soins de santé ou qui y sont reliés.

L'OUTIL DE VÉRIFICATION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Nous sommes fiers d'offrir un outil de vérification du respect de la protection des renseignements personnels (OVPRP) qui cible les dispositions de la LAIPVP et de la LRMP, cette dernière étant la première du genre au Canada à porter précisément sur les renseignements médicaux personnels. Ces lois complémentaires ont une base commune de principe de pratiques, relatives aux renseignements équitables, acceptées sur le plan international. L'OVPRP consiste en une *Liste de vérification de la protection des renseignements personnels* et en un *Guide*. Le *Guide* sert à rappeler aux utilisateurs les exigences statutaires et identifie certaines des meilleures pratiques afin d'aider à remplir la *Liste de vérification*. La *Liste de*

[2] La LRMP s'applique aux professionnels de la santé, tels que les médecins, les dentistes, les physiothérapeutes et les chiropraticiens; les établissements de soins de santé, tels que les hôpitaux, les cliniques médicales, les foyers de soins personnels, les centres de santé communautaires et les laboratoires; les agences de soins de santé qui fournissent des soins de santé en vertu d'une convention avec un dépositaire; et les organismes publics tels que décrit par la LAIPVP. Les organismes publics comprennent les services gouvernementaux provinciaux, les bureaux des ministres du gouvernement, le bureau du Conseil exécutif (le Cabinet), et les agences, y compris certains conseils, certaines commissions ou autres organismes; les organismes de gouvernements locaux, tels que la *Ville de Winnipeg*, les municipalités, les districts de gouvernement local, les districts d'aménagement et de conservation; les organismes d'éducation, tels que les conseils scolaires, les universités et les collèges; et les organismes de soins de santé, tels que les hôpitaux et les Offices régionaux de la santé.

vérification fournit aux organismes, un processus d'évaluation, étape par étape, comprenant les exigences de base pour de bonnes pratiques de protection des renseignements personnels.

L'outil de vérification de la protection des renseignements personnels vise à remplir ce que nous percevons être un écart important dans l'administration du régime de protection des renseignements personnels au Manitoba. Nous sommes, en même temps, conscients du fait que notre Bureau ne peut compromettre son rôle de bureau autonome et impartial de révision en suggérant que l'utilisation de cet outil éliminera les risques et les défauts de protection des renseignements personnels. Néanmoins, il aidera certainement les organismes à se conformer à la législation et à répondre aux exigences de diligence raisonnable. Nous encourageons l'utilisation de cet outil pour évaluer les programmes existants ou avant d'implanter de nouveaux programmes, de nouvelles pratiques, de nouveaux systèmes et initiatives qui peuvent avoir un effet sur la protection des renseignements personnels. De plus, la familiarisation avec l'OVPRP devrait aider à augmenter la sensibilisation et la compréhension des règles de gestion des renseignements personnels en vertu de la LAIPVP et de la LRMP. Il aidera aussi notre Bureau en ce qui a trait à la révision du respect de la loi.

L'outil de vérification de la protection des renseignements personnels vise à remplir ce que nous percevons être un écart significatif dans l'administration du régime de protection des renseignements personnels au Manitoba.

Afin de vous donner un avant-goût du Guide et de la Liste de vérification, nous avons joint une *Liste de vérification* en ***Annexe 1***. Ce document saisit la structure de la *Liste de vérification complète*, comprend toutes les questions et les énoncés interrogatifs du *Guide* et de la *Liste de vérification*, au complet, mais n'offre pas les notes explicatives détaillées, les commentaires, les définitions, les références statutaires ou les meilleures pratiques recommandées.

QU'EST-CE QUE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ?

La protection de la vie privée est un droit légal et de nombreuses personnes croient que c'est un droit fondamental de la personne. Au cours de la dernière décennie, ou à peu près, l'inquiétude au sujet de la protection de la vie privée a pris des dimensions complexes grandissantes, au fur et à mesure que les réseaux d'information ont augmenté exponentiellement notre capacité d'accéder aux renseignements. L'aspect précis de la protection de la vie privée qui se rapporte à la collecte, à l'utilisation, à la divulgation, au stockage et à la gestion générale des renseignements personnels est appelé la protection des renseignements personnels.

La protection de la vie privée est un droit légal et de nombreuses personnes croient que c'est un droit fondamental de la personne.

Le concept de la protection des renseignements personnels reconnaît le droit d'une personne de déterminer quand, comment et dans quelle mesure il ou elle partagera ses renseignements personnels avec d'autres.

De façon à conserver la confiance des clients, des employés, des bénéficiaires et du public, il est essentiel que le gouvernement, les organismes publics, et les dépositaires de renseignements médicaux personnels respectent la protection et la sécurité des renseignements personnels et médicaux personnels qui identifient les particuliers.

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LE SERVICE AU PUBLIC

Au cours des dernières années, nous avons noté un intérêt croissant chez les organismes publics et les dépositaires de renseignements du Manitoba dans le développement d'outil de vérification du respect de la protection des renseignements personnels ciblant précisément la législation provinciale sur l'accès et la protection des renseignements personnels. Plusieurs autres compétences ont développé des évaluations d'impact de la protection des renseignements personnels et médicaux à titre de méthodologie essentielle d'identification des questions de protection des renseignements personnels et afin de mitiger les risques et les préjudices inhérents à la collecte, à l'utilisation, à la divulgation et à la rétention des renseignements personnels au cours de la prestation de biens et services au public, dans l'environnement

d'informatique et de communications d'aujourd'hui.

Les gouvernements et les fournisseurs de soins de santé fournissent un grand éventail de services au public. Au cours de la prestation de ces services, ils obtiennent et sont les dépositaires ou ont le contrôle d'une quantité considérable de renseignements personnels et médicaux divers. Souvent, ces renseignements doivent être révélés par la personne afin de recevoir le service ou l'avantage. La nature obligatoire de telles transactions entre la personne et le fournisseur de service est régularisée par l'application de pratiques[1] d'information équitable et des lois sur la protection des renseignements personnels adoptées par la Législature du Manitoba.

En vertu de ces principes et de ces lois, « l'échange » de renseignements personnels et de renseignements médicaux personnels pour des services est enchâssé dans une relation de confiance qu'aucun renseignement personnel au-delà de ce qui est nécessaire ne sera collecté, utilisé ou divulgué afin de fournir un service ou tel que permis par la loi; que personne n'aura accès aux renseignements sauf sur une base de besoin de connaître ou tel que permis par la loi; et que les renseignements seront conservés, protégés et détruits tel qu'il est permis ou requis par la loi.

La protection de la vie privée devrait être traitée comme une partie normale, routinière et fondamentale de la planification de société et d'exploitation.

La LAIPVP et la LRMP ont été conçues pour protéger les renseignements personnels et les renseignements médicaux personnels et non pour placer des obstacles sur le chemin de l'atteinte d'objectifs corporatifs ou d'exploitation. La protection de la vie privée devrait être traitée comme une partie normale, routinière et fondamentale de la planification de société et d'exploitation. L'utilisation de cette *Liste de vérification* et du *Guide* aidera l'administration, le personnel et les agents contractuels à intégrer le respect de la protection des renseignements personnels dans le fonctionnement quotidien de leurs organismes.

...cet outil de vérification du respect de la protection des renseignements personnels n'est pas destiné à remplacer aucun outil efficace existant déjà en place, mais nous invitons tout de même les organismes publics ainsi que les dépositaires à l'utiliser à titre de mesure des outils déjà en place, ou comme leur complément.

Certains organismes publics ou dépositaires de renseignements médicaux personnels peuvent avoir des modèles d'évaluation d'impact du respect de la vie privée qu'ils utilisent, mais nous ne sommes pas informés de ce fait. De toute façon, l'outil de vérification du respect de la protection des renseignements personnels n'est pas destiné à remplacer aucun outil efficace existant déjà en place, mais nous invitons tout de même les organismes publics ainsi que les dépositaires à l'utiliser à titre de mesure des outils déjà en place, ou comme leur complément.

UN REGARD SUR LE PASSÉ AVANT DE CONTINUER

En 1999, l'Ombudsman du Manitoba a publié son premier Rapport spécial aux députés de l'Assemblée législative afin de présenter « la situation » en ce qui portait sur la protection des renseignements personnels à la suite de la proclamation de la LRMP en décembre 1997 et de la LAIPVP en mai 1998.

Lors de son adresse aux députés de l'Assemblée législative par le biais de son Rapport spécial intitulé *Arrêt sur image — La protection de la vie privée en septembre 1999*[2] l'Ombudsman écrit :

> *En raison des nombreuses questions sans précédent auxquelles s'intéressent le public, le gouvernement et notre Bureau en matière de protection de la vie privée, et étant donné leur complexité et leur carac-*

[1] En 1996, l'Association canadienne de normalisation a lancé un Code canadien sur la protection des renseignements personnels et subséquemment l'a adopté à titre de « norme canadienne ». Ce code est résumé en Annexe 2 de ce Rapport spécial. Il offre beaucoup de l'infrastructure de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ), qui a reçu la sanction royale en l'an 2000. Cette loi entrera en vigueur le 1er janvier 2004, en ce qui a trait à la collecte, l'utilisation et la divulgation de renseignements personnels dans le cours de toute activité commerciale au Manitoba, y compris les organismes réglementés par la province en l'absence de législation « substantiellement similaire ».

[2] Notre Rapport spécial aux députés de l'Assemblée législative Arrêt sur image. La protection de la vie privée en septembre 1999, offre des renseignements et des commentaires sur l'environnement général de la protection de la vie privée jusqu'en l'année 2000, et est affiché sur notre site Web à l'adresse : http://www.ombudsman.mb.ca/reports/snapshot.htm

tère dynamique, nous avons préparé ce rapport spécial qui présente un arrêt sur image de la situation actuelle en matière de protection de la vie privée.

Lorsque nous regardons les quelques cinq années depuis l'entrée en vigueur de la LAIPVPP et de la LRMP, les mots de l'écrivain du 19e siècle, Alphonse Karr nous viennent à l'esprit en ce qui a trait à notre premier Rapport spécial : « Plus ça change, plus c'est la même chose. »

Le 11 septembre 2001

Au cours des dernières années, les attaques terroristes du 11 septembre 2001, aux États-Unis, ont mis en lumière, plus qu'aucun autre événement, les tensions entre les droits et libertés civils et les besoins de sécurité publique et nationale.

Au cours des dernières années, les attaques terroristes du 11 septembre 2001, aux États-Unis, ont mis en lumière plus qu'aucun autre événement, les tensions entre les droits et libertés civils et les besoins de sécurité publique et nationale. Toutefois, attribuer l'état instable ou — comme le dirait d'aucun — conflictuel de la protection des droits à la vie privée à ces attaques ne reconnaîtrait pas que beaucoup de ces questions en étaient déjà rendues à un niveau important d'exposition nationale et internationale.

Au début des années 1970, l'utilisation de ce que l'on nommait fréquemment « le traitement de données » se répandait rapidement dans les organismes des secteurs publics et privés. Certaines des répercussions de cette technologie sur la protection de la vie privée, ont été réalisées très tôt en Amérique et en Europe. À la même période, la convergence et l'intégration des technologies de diffusion fixes comprenant des capacités de traitement de données étaient déjà bien engagées, incarnées d'une certaine manière, par l'Internet d'aujourd'hui, qui est passé d'un réseau limité à un réseau ouvert pour la transmission de renseignements.

En 1980, l'Organisation de coopération et de développement économiques (OCDE) a présenté les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, que le Canada a acceptés, en 1984. Ces lignes directrices établissent ce qui est maintenant connu comme les principes de pratique équitable en ce qui a trait aux renseignements, qui sont au cœur des lois modernes sur la protection de la vie privée et des renseignements personnels, au Canada et ailleurs.

Les événements du 11 septembre ont intensifié et non pas introduit les inquiétudes maintenant familières au sujet de la découverte d'une relation raisonnable entre le droit à la vie privée et la sécurité publique ou les affaires de sécurité dans l'utilisation des technologies modernes d'information et de communication.

En l'an 2000, la relation entre les technologies d'information et de communication et les questions de vie privée est devenu un sujet qui présente de nombreux aspects, au centre d'une discussion internationale, et d'un débat animé et souvent amer, particulièrement en relation avec leur utilisation actuelle, ou possible, à des fins de surveillance. Les événements du 11 septembre ont intensifié et non pas introduit les inquiétudes maintenant familières au sujet de la découverte d'une relation raisonnable entre le droit à la vie privée et la sécurité publique ou les affaires de sécurité dans l'utilisation des technologies modernes d'information et de communication.

Dans cette perspective [de mondialisation], presque toutes choses peuvent être perçues comme liées entre elles et l'information n'a pas de frontière qu'elles soient géopolitiques ou technologiques.

Les technologies d'information et de communication et de meilleurs services

Pour la plus grande partie des trois dernières décennies, le développement rapide et accéléré des technologies de traitement de l'information et des communications a établi les normes pour la caractéristique sociale, culturelle, politique et économique définissant notre présent : la mondialisation.[1] Dans cette perspective mondiale, presque toutes choses peuvent être perçues comme liées entre elles et l'information n'a pas de frontière qu'elles soient géopolitiques ou technologiques.

[1] Ce concept complexe et à dimensions multiples a été défini par le gouvernement canadien comme décrivant « la mobilité accrue des biens, des services, de la main d'œuvre, de la technologie et des capitaux de par le monde. Quoique la mondialisation ne soit pas un nouveau développement, sa vitesse a augmenté avec l'arrivée des nouvelles technologies, particulièrement dans le secteur des télécommunications. » (Voir http://canadianeconomy.gc.ca/english/economy/globalization.html)

Les organismes, y compris les gouvernements, ont reconnu et réagi depuis longtemps à une variété de pressions pour offrir leurs biens et services de manière plus efficace et plus utile. La meilleure utilisation de l'information a souvent été vantée comme étant la clé maitresse de meilleurs services. Au cours des récentes décennies, le développement rapide et envahissant des technologies d'information et de communication (TCI) a été décrit comme exerçant une « poussée » irrésistible vers une plus grande utilisation de technologies elles-mêmes, avec des applications pour des objectifs d'affaire et de logiciel qui fournissent une « poussée » plus intense ou renforcée.

Il n'y a aucun doute que les TCI ont déjà apporté des avantages importants pour la prestation de services publics dans le domaine de la santé, de l'éducation, de l'aide sociale, de l'agriculture, du milieu de travail, de l'environnement et dans le maintien de la paix, pour n'en nommer que quelques-uns. De nombreux fournisseurs de services croient que ces accomplissements ne sont que les débuts de l'exploration ou les présages d'applications futures des TCI qui amélioreront la prestation de services.

... la pression est persuasive pour utiliser les renseignements d'identification personnels comme la méthode essentielle de s'y retrouver et d'utiliser la grande quantité de données disponibles.

La « volonté » ou la « nécessité » d'utiliser les renseignements d'identification personnels

Dans cette situation dynamique, où, d'une façon ou d'une autre, les personnes sont au centre des raisons pour l'existence des organismes, la pression est intense pour utiliser les renseignements d'identification personnels comme la méthode essentielle de s'y retrouver et d'utiliser la grande quantité de données disponibles. Même au niveau actuel de développement des technologies de communication et de traitement de données, il ne semble plus être tiré par les cheveux de croire que bientôt toute partie aléatoire de renseignement enregistrée et transmise au sujet de qui que ce soit, n'importe où, pourrait être colliger à d'autres parties et expédiée n'importe où, afin de fournir un portrait complet de cette personne, dans un dossier ou en temps réel.

[La]... concentration de renseignements [électroniques] souligne le besoin irrésistible et urgent qu'on les organismes d'être en contrôle complet de leur collection de renseignements personnels, de son utilisation, de sa divulgation et de sa rétention et de leurs pratiques de sécurité.

L'immense volume de renseignements personnels qui est déjà géré de manière électronique par les systèmes de soins de santé et les secteurs publics au Canada nécessiterait littéralement des vingtaines d'entrepôts d'archives, si on les gardait sur papier — plus probablement des centaines. Cette concentration spatiale de renseignements souligne le besoin irrésistible et urgent qu'ont les organismes d'être en contrôle complet de leur collecte de renseignements personnels, de leur utilisation, de leur divulgation et de leur rétention ainsi que de leurs pratiques de sécurité. Autrement les risques d'infraction à la protection de la vie privée sont augmentés de manière importante comparés à ceux des dossiers sur papier.

L'établissement d'un [réseau électronique pancanadien de renseignements médicaux personnels]...a été le sujet d'études et de recommandation depuis un certain nombre d'années et semble être sur le point de se réaliser véritablement .... La confiance du public dans la protection des renseignements personnels, sous-tendant le projet, sera un facteur habilitant clé dans le succès de ce projet.

Déjà, les gouvernements fédéral et provinciaux partout au Canada utilisent, mettent en application ou examinent les TCI dans le but avoué de fournir des services améliorés, plus économiques et plus efficaces dans la plupart des secteurs de leurs compétences. Un exemple particulièrement remarquable est le développement éventuel d'archives électroniques pancanadiens de renseignements médicaux.[9] L'établissement d'un tel réseau de renseignements médicaux a été le sujet d'études et de recommandations depuis un certain nombre d'années et semble être sur le point

[9] Le Manitoba était en tête de file des gouvernements du Canada à entreprendre un projet d'envergure afin d'établir un réseau de renseignements médicaux. Annoncé en 1994, il a été annulé en 2000 sans avoir atteint son principal objectif de fournir un accès plus rapide et plus facile, à une plage importante de renseignements vitaux pour les bénéficiaires, aux fournisseurs de soins de santé. Le développement éventuel d'un réseau manitobain de renseignements médicaux était le motif premier de la distinction du Manitoba d'avoir adopter le premier statut au pays portant sur les renseignements médicaux personnels : la Loi sur les renseignements médicaux personnels. Notamment, la quatrième division du préambule de la Loi se lit comme suit : « l'établissement de règles claires et certaines touchant la collecte, l'utilisation et la communication des renseignements médicaux personnels constitue un soutien essentiel aux systèmes d'information électroniques en matière de santé, lesquels systèmes peuvent améliorer tant la qualité des soins donnés aux patients que la gestion des ressources dans le domaine des soins de santé ».

de se réaliser véritablement. Le coût se chiffrant dans les milliards de dollars, nous pouvons nous attendre à ce que le développement de ce réseau soit le sujet de consultations et de discussions publiques importantes dans l'avenir immédiat.

La confiance du public dans la protection des renseignements personnels, sous-tendant le projet, sera un facteur habilitant clé dans le succès de ce projet. Au cœur de la perspective publique, se retrouvera l'assurance que toutes les parties concernées dans le réseau de renseignements médicaux personnels respectent les lois, les principes et les politiques sur la collecte, l'utilisation, la divulgation, la rétention et la sécurité des renseignements médicaux personnels utilisés.

LA DILIGENCE RAISONNABLE ET LA GESTION DU RISQUE

Entre autres choses, la vérification du respect de la protection des renseignements personnels est un outil efficace de diligence raisonnable et de gestion du risque qui exige une direction et un engagement du palier de direction des organismes. Alors que le besoin de vérification peut être identifié à tous les paliers organisationnels, le produit fini devrait être de fournir les résultats de l'évaluation aux gestionnaires pour la révision, la signature et la prise de décision de toutes actions ou directives qui en découlent, fermant ainsi la boucle de la responsabilité.

Entre autres choses, la vérification du respect de la protection des renseignements personnels est un outil efficace de diligence raisonnable et de gestion du risque qui exige une direction et un engagement du palier de direction des organismes.

Effectuer une vérification du respect de la protection des renseignements personnels au cours des premiers stades de développement ou de la modification d'un programme, d'une practique, d'un système ou de la législation peut aider à s'assurer que les exigences de protection de la vie privée sont identifiées et remplies à point donné et d'une manière rentable...

Cet outil de respect de la protection des renseignements personnels peut être utilisé à titre d'assise pour évaluer le respect de la protection de programmes existants. Il est particulièrement opportun de faire une vérification lorsqu'un nouveau programme, une nouvelle pratique, un nouveau système d'information ou une nouvelle législation est en développement ou est modifié, si ce programme ou ce système collecte, stocke, utilise ou divulgue des renseignements personnels ou des renseignements médicaux personnels. Effectuer une vérification du respect de la protection des renseignements personnels au cours des premiers stades de développement ou de la modification d'un programme, d'une practique, d'un système ou de la législation peut aider à s'assurer que les exigences de protection de la vie privée sont identifiées et remplies à point donné et d'une manière rentable, que des initiatives envahissantes de la vie privée ne sont pas mises en application, que les atteintes à la protection de la vie privée sont évitées dans la mesure du possible, et que les organismes n'aient pas à entreprendre des vérifications coûteuses ou même annuler une initiative dispendieuse après sa mise en application.

LES RISQUES ASSOCIÉS AU DÉFAUT D'EXÉCUTER UNE VÉRIFICATION DU RESPECT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les risques généraux associés au défaut d'entreprendre une vérification systématique du respect de la protection des renseignements personnels sont habituellement catégorisés comme suit :

- Tout d'abord, il y a le risque pour les renseignements personnels des individus sachant qu'une fois que la protection de la vie privée est perdue, elle ne peut généralement pas être recouvrée.
- Le programme ou l'initiative législative peut être discrédité apportant ainsi une perte importante, et quelquefois cruciale, de la confiance du public dans l'importance ou la considération qu'un organisme accorde aux droits légaux du public.
- Les systèmes électroniques, en particulier, mais aussi les programmes peuvent devoir être réévalués, modifiés ou convertis à des coûts importants.
- Les renseignements personnels ou les renseignements médicaux personnels sont divulgués ou «

partagés » par le biais d'ententes qui peuvent ne pas respecter la législation ou les « meilleures pratiques », ou sans aucune entente écrite.

- Des exigibilités peuvent s'en suivre pour les employés et l'organisme.

L'UTILISATION DE L'OUTIL DE VÉRIFICATION DU RESPECT DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Entreprendre une vérification complète du respect de la protection des renseignements personnels exige habituellement un engagement de la part de l'organisme impliqué. Pour cette raison, nous répétons l'importance d'obtenir la direction de palier supérieur de l'administration dès le début, gardant en tête que les résultats devraient être signés par les décideurs administratifs.

Une révision en profondeur du respect des exigences légales peut être une tâche onéreuse dont le degré de difficulté sera influencé par un certain nombre de facteurs, au-delà de l'engagement des cadres supérieurs à des pratiques d'information équitables. Ceux-ci comprennent l'expertise en protection des renseignements personnels dont l'organisme dispose ou à laquelle il a accès; l'ampleur à laquelle les renseignements personnels et les renseignements médicaux personnels sont collectés, utilisés et divulgués par les programmes ou les systèmes d'information; la délicatesse des renseignements visés; la qualité, le cours et l'envahissement de la tenue de registres adéquats et de pratiques de gestion des renseignements; et de l'amplitude de l'exploitation ou des programmes impliqués.

L'utilisation de la Liste de contrôle aidera les entreprises à rendre conforme les programmes, les pratiques, les activités et les systèmes d'information qui ne répondent pas aux exigences de la législation sur la protection des renseignements personnels.

L'utilisation de la Liste de contrôle aidera les organismes soumis à la LAIPVP et à la LRMP à identifier les politiques, les processus et les structures organisationnelles qui ne répondent pas aux exigences de la législation, et à développer la planification afin de rendre les programmes, les pratiques, les activités et les systèmes d'information, qui ne respectent pas la législation, conformes aux exigences de respect de la protection des renseignements personnels.

La *Liste de contrôle* contient des contreparties pour évaluer le respect de la protection des renseignements personnels et peut être utilisée par le Bureau de l'Ombudsman à titre de lignes directrices pour des vérifications et des enquêtes. L'utilisation d'un processus d'évaluation d'impact de la protection des renseignements personnels aidera à minimiser les infractions à la protection des renseignements personnels, mais elle peut ne pas éliminer le risque entièrement, même si le plan général d'un programme ou d'une proposition législative semble respecter les exigences statutaires. Des infractions précises se produiront, malheureusement, de temps à autre et devront être réglées sur une base de cas par cas. Néanmoins, un contrôle ou une enquête du respect de la protection des renseignements, par le Bureau de l'Ombudsman, tiendra compte du degré de diligence raisonnable qui a été mis en pratique par le biais de l'utilisation d'une évaluation d'impact sur la protection des renseignements personnels.

Annexe 1

OUTIL DE VÉRIFICATION DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

LISTE DE CONTRÔLE EN UN CLIN D'ŒIL

INTRODUCTION

Ce document, qui est une forme abrégée de la plus grande. Liste de vérification, a pour objectif de fournir aux utilisateurs un bref aperçu des questions posées au cours du processus d'évaluation. Il permettra de plus facilement enregistrer les réponses et d'évaluer globalement jusqu'à quel point les lois sont respectées.

TABLE DES MATIÈRES

ÉLÉMENT 1: Déterminer les objectifs et limiter la collecte de renseignements personnels et de renseignements médicaux personnels 16

ÉLÉMENT 2: Limiter l'utilisation, la divulgation et la conservation de renseignements personnels et de renseignements médicaux personnels..... 17

ÉLÉMENT 3: Garantir l'exactitude des renseignements personnels et des renseignements médicaux personnels 20

ÉLÉMENT 4: Protéger des renseignements personnels et des renseignements médicaux personnels 21

ÉLÉMENT 5: Garantir l'accès individuel aux renseignements personnels et aux renseignements médicaux personnels 23

ÉLÉMENT 6: Plaintes posées en raison du non-respect des lois 23

ÉLÉMENT 7: Responsabilité et transparence en matière de politiques et de pratiques 24

ÉLÉMENT 8: Évaluer les risques concernant la prestation de services électroniques 25

ÉLÉMENT 1

DÉTERMINER LES OBJECTIFS ET LIMITER LA COLLCTE DE RENSEIGNEMENTS PERSONNELS ET DE RENSEIGMENTS MÉDICAUX PERSONNELS

N° LÉGENDE[7]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

		Expl?		NE/PA?	
	O	N	O	N	O	N
1. Il existe une description détaillée du type de renseignements personnels, de renseignements médicaux personnels ou de données personnelles à recueillir dans le cadre de ce programme ou de cette initiative.						
2. La collecte de ces renseignements personnels est autorisée en vertu de la LAIPVP, pour l'une des raisons suivantes :†						
a. elle est autorisée en vertu d'un texte législatif provincial ou fédéral;						
b. elle est nécessaire dans le cadre d'un programme ou d'une activité de l'organisme publique, et y est directement liée;						
c. elle est indispensable aux fins de l'exécution de la loi ou de la prévention du crime.						
3. La collecte de *renseignements médicaux personnels* n'est autorisée que dans les cas suivants :						
a. elle est destinée à une fin légitime ayant trait au travail ou aux activités du dépositaire;						
b. elle est nécessaire à l'accomplissement du travail ou des activités du dé positaire.						
4. Les *renseignements personnels* ou des *renseignements médicaux personnels* sont recueillis uniquement auprès de la personne concernée ou auprès de son représentant personnel.						
5. Si des renseignements personnels ou des renseignements médicaux personnels sont recueillis indirectement (c.-à-d., auprès d'un tiers), leur collecte indirecte est autorisée en vertu soit du paragraphe 37(1) de la LAIPVP, soit de l'article 14 de la LRMP.						
6. Les personnes concernées sont informées (avisées) des fins auxquelles les renseignements sont destinés, de la disposition législative permettant leur collecte (dans le cadre de la LAIPVP) et de la manière de prendre contact avec le cadre ou l'employé apte à les renseigner sur la collecte de ces renseignements.						

† REMARQUE: Veuillez indiquer la réponse pertinente, soit (a), (b) ou (c). Si vous choisissez la réponse (a), prière d'indiquer le nom de la loi (ou des lois) et les dispositions législatives s'y rapportant.

[7] Les notes explicatives offrent des renseignements supplémentaires sur ce qui existe (p. ex. une politique de sécurité), tandis que les plans d'action donnent des précisions sur les mesures de correction ou de développement qu'il faudrait prendre (p. ex. l'élaboration d'un programme de formation pour permettre la sensibilisation du personnel à la sécurité et la protection de la vie privée).

ÉLÉMENT 2

LIMITER L'UTILISATION, LA DIVULGATION ET LA CONSERVATION DE RENSEIGNEMENTS PERSONNELS ET DE RENSEIGNEMENTS MÉDICAUX PERSONNELS

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

		Expl?		NE/PA?	
	O	N	O	N	O	N
A. Limiter l'utilisation de *renseignements personnels* et de *renseignements médicaux personnels*						
1. *Les renseignements personnels* ou les *renseignements médicaux personnels* ne servent qu'aux fins auxquelles ils ont été recueillis ou qu'à une utilisation conforme à ces fins, en vertu de la *LAIPVP*, ou directement liée à ces fins, en vertu de la *LRMP*.						
2. On obtient le consentement de la personne concernée avant d'utiliser ses *renseignements personnels* pour des fins qui ne sont PAS conformes au but original ou, dans le cas de *renseignements médicaux personnels*, pour des fins qui ne sont PAS directement liées au but original, lequel a nécessité leur collecte.						
3. Il existe une liste du personnel ou des services qui utilisent cette collecte de *renseignements personnels* ou de *renseignements médicaux personnels*.						
4. Il existe des systèmes de surveillance (physique, administratif ou technique) pour que l'accès aux *renseignements personnels* et aux *renseignements médicaux personnels* identifiables soit limité uniquement aux personnes qui doivent en prendre connaissance.						
5. On ne recueille que le minimum de *renseignements personnels* ou de *renseignements médicaux personnels* nécessaires pour réaliser la fin visée.						
6. Les *renseignements personnels* ou les *renseignements médicaux personnels* sont utilisés à la fin visée, de manière à garder le plus d'anonymat possible.						
B. Limiter la divulgation de *renseignements personnels* et de *renseignements médicaux personnels*						
1. On obtient le consentement de la personne concernée avant de communiquer des *renseignements personnels* ou des *renseignements médicaux personnels* à un autre ministère ou organisme gouvernemental, organisme public local, dépositaire ou tiers.						
2. S'il n'est pas possible d'obtenir le consentement de la personne concernée, la divulgation est autorisée en vertu d'une disposition particulière du paragraphe 44(1) de la *LAIPVP* ou du paragraphe 22(2) de la *LRMP*.						
3. Lorsqu'il est nécessaire de communiquer des *renseignements personnels*, la quantité et le type de renseignements est communiqué uniquement aux personnes ayant besoin de les connaître.						
4. La *divulgation* des renseignements se fait de manière à garder le plus d'anonymat possible, tout en répondant aux besoins du destinataire.						
5. Le personnel conserve un registre ou une piste de vérification permetant de connaître : a. les renseignements qui ont été communiqués, b. la ou les personnes à qui ils ont été communiqués; c. pourquoi ces renseignements ont été communiqués et qui a autorisé leur *divulgation*.						

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

	Expl?		NE/PA?	
	O	N	O	N	O	N

C. Utilisation et divulgation des renseignements personnels qui ne sont pas autorisés autrement en vertu de la Section 3 de la LAIPVP.

1. **Pour un organisme public autre** qu'un organisme public local en vertu de l'article 46 de la LAIPVP :
   La demande a été renvoyée au Comité d'évaluation afin d'obtenir son avis :
   a. si l'utilisation ou la divulgation des renseignements que l'on propose n'est pas autorisée autrement en vertu de la Section 3 et nécessite le couplage de banques de renseignements ou l'appariement de renseignements personnels se trouvant dans deux banques de renseignements; ou
   b. si l'on reçoit une demande de divulgation en nombre de renseignements personnels qui se trouvent dans un répertoire public ou dans une autre collecte de renseignements personnels.
2. Renseignements personnels recueillis **pour un organisme public local** en vertu de l'article 46 de la LAIPVP :
   La demande a été évaluée par l'organisme public local ou encore envoyée au Comité d'évaluation afin d'obtenir son avis :
   a. si l'utilisation ou la divulgation des renseignements que l'on propose n'est pas autorisée autrement en vertu de la Section 3 et nécessite le couplage de banques de renseignements ou l'appariement de renseignements personnels se trouvant dans deux banques de renseignements; ou
   b. si l'on reçoit une demande de divulgation en nombre de renseignements personnels qui se trouvent dans un répertoire public ou dans une autre collecte de renseignements personnels.
3. Quant à l'utilisation ou à la divulgation de renseignements personnels proposée en vertu de l'article 46 de la LAIPVP, le responsable de l'organisme public ou de l'organisme public local a examiné l'avis du comité d'évaluation et a approuvé les conditions devant être remplies en vertu du paragraphe 46(6), y compris la conclusion d'un accord écrit avec le destinataire des renseignements personnels.

D. Divulgation de renseignements personnels à des fins de recherche en vertu de la LAIPVP.

1. Le responsable de l'organisme public ou de l'organisme public local a examiné l'avis reçu du comité d'évaluation et a approuvé les conditions devant être remplies en vertu du paragraphe 47(4), y compris la conclusion d'un accord écrit avec le destinataire des renseignements personnels.

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

		Expl?		NE/PA?	
	O	N	O	N	O	N
E. Divulgation de renseignements médicaux personnels pour les besoins d'un projet de recherche, en vertu de la *LRMP*						
1. Les *renseignements médicaux personnels* requis pour un projet de recherche sont des renseignements consignés concernant un particulier identifiable et ayant trait :						
a. à sa santé ou à son dossier médical, y compris les renseignements d'ordre génétique le concernant;						
b. aux soins de santé qui lui sont fournis;						
c. au paiement des soins de santé qui lui sont fournis, notamment						
d. le numéro d'identification médical personnel (NIMP) et tout numéro ou symbole, ou toute autre indication identificatrice, qui est propre au particulier;						
e. les renseignements identificateurs concernant le particulier qui sont recueillis à l'occasion de la fourniture de soins de santé ou du paiement de ces soins et qui découlent de ces opérations.						
2. Le projet de recherche a été approuvé conformément aux exigences de l'article 24 de la *LRMP* par :						
a. le Comité de la protection des renseignements médicaux (CPRM) si le gouvernement ou un organisme gouvernemental conserve les *renseignements médicaux personnels*;						
b. un comité de révision de la recherche institutionnelle, si les renseignements personnels sont conservés par un dépositaire autre que le gouvernement ou un organisme gouvernemental.						
3. La personne qui se propose de réaliser le projet de recherche et le *dépositaire*, conformément au paragraphe 24(4) de la *LPRP* et à ses règlements d'application, concluent un accord dans lequel la personne consent :						
a. à ne pas publier les *renseignements médicaux personnels* demandés sous une forme qui pourrait vraisemblablement permettre d'identifier les particuliers concernés;						
b. à n'utiliser les *renseignements médicaux personnels* demandés qu'aux fins visées par le projet de recherche approuvé,						
c. à s'assurer que suffisamment de mesures de sécurité sont en place pour protéger la sécurité et la confidentialité des *renseignements médicaux personnels*;						
d. à s'assurer que les renseignements seront détruits ou dépersonnalisés dans les plus brefs délais, conformément aux fins du projet.						
F. Limiter la conservation de renseignements personnels :						
1. Il existe une politique écrite en matière de dossiers et de rétention des données conforme à toutes les dispositions de la législation.						
2. *Les renseignements personnels* et *les renseignements médicaux personnels* utilisés pour prendre une décision ayant une incidence directe sur un particulier sont conservés pendant une période de temps raisonnable afin de permettre à la personne d'y avoir accès.						

ÉLÉMENT 3

GARANTIR L'EXACTITUDE DES RENSEIGNEMENTS PERSONNELS ET DES RENSEIGNEMENTS MÉDICAUX PERSONNELS

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

	Expl?		NE/PA?	
	O	N	O	N	O	N
1. Il y a en place des procédés qui permettent de vérifier les *renseignements personnels* et les *renseignements médicaux personnels* et de gérer les demandes de correction, conformément aux articles 38 et 39 de la *LAIPVP* et aux articles 12 et 16 de la *LRMP*.						
2. La personne autorisée à modifier ou à corriger les *renseignements personnels* ou les *renseignements médicaux personnels* est clairement désignée de manière qu'aucune autre personne non autorisée ne puisse y apporter des modifications ou des corrections.						
3. Il existe une piste de vérification qui permet de savoir quand un document ou un dossier a été établi ou mis à jour, et d'identifier la personne qui l'a fait.						

ÉLÉMENT 4

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DES RENSEIGNEMENTS MÉDICAUX PERSONNELS

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

			Expl?		NE/PA?	
	O	N	O	N	O	N
1. Il y a en place des mesures de sécurité pour protéger les renseignements personnels et les renseignements médicaux personnels quel que soit leur format (c.-à-d. sur papier, documents photographiques, électroniques, etc.).						
2. Les politiques de sécurité comprenant des renseignements écrits incluent notamment une définition des rôles et des responsabilités, ainsi que des sanctions à prendre en cas de non-respect des politiques.						
3. Le personnel reçoit de la formation contenue au sujet des politiques et des mesures de sécurité, et est informé régulièrement de l'importance des éléments de sécurité et de confidentialité.						
4. Toute atteinte ou violation à la sécurité est documentée et réglée selon les procédés en place.						
5. L'accès aux renseignements personnels ou aux renseignements médicaux personnels est régulièrement contrôlé et vérifié.						
6. *Les renseignements personnels* et les *renseignements médicaux personnels* sont stockés ou entreposés dans un endroit physiquement sécuritaire.						
7. *Les renseignements personnels et les renseignements médicaux personnels,* quel que soit leur format, sont éliminés de manière sécuritaire afin d'éviter que toute personne non autorisée ne puisse y avoir accès.						
8. Lorsque les renseignements personnels et les renseignements médicaux personnels, quel que soit leur format, sont physiquement enlevés d'une zone d'accès réservée, cela se fait selon les procédés en place et de manière à garantir la sécurité des renseignements à tout moment.						

N[1] LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

			Expl?		NE/PA?	
	O	N	O	N	O	N
Sécurité des systèmes électroniques :						
1. Les utilisateurs doivent avoir un code d'utilisateur et un mot de passe pour accéder aux renseignements personnels et aux renseignements médicaux personnels, et les mots de passe sont changés régulièrement.						
2. Les cotes de sécurité pour accéder au réseau et aux applications sont attribuées selon un principe d'accès sélectif, en fonction des exigences particulières de connaissances des différents postes au sein de l'organisme.						
3. Les permissions d'accès sont annulées rapidement au besoin (p. ex. lorsqu'un employé quitte son poste ou déménage).						
4. Les systèmes contiennent des pistes de vérification pour contrôler l'accès aux renseignements ainsi que des registres permettant de connaitre toute utilisation anormale ou inhabituelle.						
5. Les listes de contrôle et les pistes de vérification sont examinées régulièrement.						
6. Les renseignements personnels et les renseignements médicaux personnels sont transmis de manière sécuritaire afin de minimiser tout risque d'une interception non autorisée ou accidentelle par un tiers.						
7. Au besoin, une protection antivirus est mise en application et un coupe-feu est en place, pour tous les systèmes d'information contenant des renseignements personnels ou des renseignements médicaux personnels.						
8. Les fournisseurs externes chargés des services de gestion et de technologie de l'information sont couverts par un accord écrit qui prévoit leur protection contre des risques tels que l'accès, l'utilisation, la divulgation, la conservation ou la destruction non autorisé, et ce, conformément au paragraphe 44(2) de la LAIPVP et au paragraphe 25(3) de la LRMP.						

ÉLÉMENT 5

GARANTIR L'ACCÈS INDIVIDUEL AUX RENSEIGNEMENTS PERSONNELS ET AUX RENSEIGNEMENTS MÉDICAUX PERSONNELS

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

			Expl?		NE/PA?	
	O	N	O	N	O	N
1. Il y a en place un processus pour répondre aux demandes d'accès en vertu des dispositions législatives.						
2. Les particuliers sont informés que l'organisme possède des renseignements personnels ou des renseignements médicaux personnels à leur sujet, et qu'ils peuvent y avoir accès, sauf dans des circonstances limitées, tel qu'il est défini dans la loi.						
3. On donne suite (soit gratuitement, soit en exigeant des frais minimes) aux demandes d'accès aux renseignements, dans les délais prescrits et conformément aux dispositions législatives.						
4. Les renseignements demandés sont fournis dans un format compréhensible et l'organisme se tient à la disposition du demandeur, le cas échéant, pour expliquer des termes ou des abréviations.						
5. Si l'on refuse de donner accès à des renseignements personnels ou à une partie de ceux-ci, le demandeur est informé clairement de la raison pour laquelle cela lui a été refusé.						

ÉLÉMENT 6

PLAINTES POSÉES EN RAISON DU NON-RESPECT DES LOIS

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

			Expl?		NE/PA?	
	O	N	O	N	O	N
1. Il y a en place des politiques et des procédures en ce qui concerne la divulgation de renseignements personnels afin de s'assurer que les particuliers sont régulièrement informés du fait qu'ils peuvent déposer une plainte auprès de l'organisme et qu'ils ont légalement le droit de déposer une plainte auprès de l'ombudsman du Manitoba relativement à leurs droits en matière de renseignements personnels et de renseignements médicaux personnels.						

ÉLÉMENT 7

RESPONSABILITÉS ET TRANSPARENCE EN MATIÈRE DE POLITIQUES ET DE PRATIQUES

N° LÉGENDE[1]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

			Expl?		NE/PA?	
	O	N	O	N	O	N
1. Le personnel de l'organisme comprend que c'est le chef d'un ministère du gouvernement provincial, d'un organisme gouvernemental ou d'un organisme public local, ou encore un dépositaire qui est responsable de l'observation des lois sur l'accès à l'information et la protection de la vie privée, et que toute délégation de pouvoirs ou de tâches doit être enregistrée officiellement.						
2. Un ou des employés au sein de l'organisme sont formellement chargés d'assurer, au jour le jour, le respect des dispositions législatives sur l'accès à l'information et la protection de la vie privée (il s'agit d'un « coordonnateur chargé de l'accès à l'information et de la protection de la vie privée », en vertu de la LAIPVP, et d'un « fonctionnaire chargé de la protection des renseignements médicaux personnels », en vertu de la LRMP). L'identité de ces personnes est connue par tout le personnel de l'organisme.						
3. Il existe des politiques et des procédures écrites qui définissent les responsabilités de la personne chargée de protéger les renseignements personnels et les renseignements médicaux personnels.						
4. Le personnel approprié a accès à des séances de formation continue pour être apte à mettre en œuvre les politiques et les procédures concernant l'accès à l'information et la protection de la vie privée.						
5. D'autres parties telles que des gestionnaires de l'information ou des préposés aux renseignements, qui pourraient être autorisés à avoir accès aux renseignements personnels ou aux renseignements médicaux personnels en vertu des parties 3 de la LAIPVP ou de la LRMP, connaissent les politiques et les procédures connexes en ce qui a trait aux renseignements personnels et les respectent.						
6. Les particuliers peuvent aisément obtenir des renseignements au sujet des politiques et des procédures relatives à la protection des renseignements personnels.						
7. En vertu de la LAIPVP, les fichiers de renseignements personnels ont été établis et décrits. Ils sont de plus régulièrement mis à jour et disponibles au public, au besoin. (Il est à noter que la LRMP ne possède pas de disposition semblable relative à la préparation d'un répertoire, y compris une description des fichiers de renseignements personnels.)						
8. En vertu de la LAIPVP et dans le cas d'un organisme public qui n'est pas un organisme public local, il faut (1) conserver un document faisant état de l'utilisation et de la divulgation des renseignements personnels qui ne sont pas inclus dans le répertoire, (2) annexer ou incorporer cette information aux renseignements personnels et (3) avoir en place un processus pour que cette information figure au répertoire. (Il est à noter que la LRMP ne possède pas de disposition exactement semblable.)						
9. Il existe un processus pour répondre aux questions et aux préoccupations concernant la protection des renseignements personnels.						

ÉLÉMENT 8

ÉVALUER LES RISQUES CONCERNANT LA PRESTATION DE SERVICES ÉLECTRONIQUES (PSÉ)

N° LÉGENDE[8]:

« **O** » = Oui; « **N** » = Non; « **Expl?** » = Explanation?;
« **NE/PA?** » = Note explicative ou plan d'action?

		Expl?		NE/PA?	
		O	N	O	N	O	N
1.	Existe-t-il des diagrammes pour illustrer la circulation de renseignements personnels et de renseignements médicaux personnels pour ce projet?						
2.	Une personne a-t-elle été désignée responsable du contrôle et de la protection de tous les renseignements personnels et renseignements médicaux personnels traités par le système de PSÉ?						
3.	Si les transactions de plus d'un programme, organisme ou ministère seront traitées par le système PSÉ, est-ce que l'intégration des données sera soumise à certaines contraintes?						
4.	Si ce projet de PSÉ exige l'utilisation d'identificateurs communs ou d'une infrastructure d'identification commune, a-t-on envisagé la prise de mesures pour assurer une meilleure protection des renseignements personnels, de manière à éviter tout risque de porter atteinte à la vie privée?						
5.	Ce projet de PSÉ exigera-t-il un appariement de données (l'établissement de profils) ou un couplage de données?						
6.	Existe-t-il, au besoin, un moyen d'obtenir le consentement des personnes par voie électronique et de vérifier, d'enregistrer et de gérer cette information grâce à l'informatique?						
7.	A-t-on envisagé, pour ce projet de PSÉ, l'utilisation de technologies ou de techniques particulières pour assurer une meilleure protection de la vie privée?						
8.	A-t-on cerné et documenté tous les risques qui pourraient porter atteinte à la vie privée pendant le déroulement du projet?						
9.	A-t-on fait le nécessaire pour minimiser ou éviter ces risques?						
10.	A-t-on réalisé, pour tous les aspects du système PSÉ, une analyse complète des risques pour déterminer les exigences en matière de vérification régulière auxquelles il faut satisfaire, ainsi que les mesures de contrôle appropriées et continues qu'il faudrait prendre pour assurer la protection des renseignements personnels et des renseignements médicaux personnels, notamment ceux des utilisateurs finaux?						
11.	A-t-on consulté les intervenants clés au sujet des risques que ce projet risque de poser quant à la protection de la vie privée?						
12.	S'il n'a pas été possible d'éliminer tous les risques en ce qui concerne la protection de la vie privée, a-t-on formulé une stratégie pour répondre aux préoccupations du public?						
13.	Les fournisseurs de services électroniques les a-t-on soumis à des contraintes quant à la collecte, à l'utilisation et à la divulgation de renseignements personnels, conformément à la LAIPVP et à la LRMP?						
14.	Les contrats conclus pour les besoins du projet contiennent-ils tous des dispositions en matière de protection des données?						

[8] On demande aux utilisateurs de fournir des notes explicatives ou des plans d'action pour TOUTES les questions posées dans cet élément, quelle que soit la réponse fournie. Les notes explicatives offrent des renseignements supplémentaires sur ce qui existe (p. ex. une politique de sécurité), tandis que les plans d'action donnent des précisions sur les mesures de correction ou de développement qu'il faudrait prendre (p. ex. l'élaboration d'un programme

Annexe 2

PRINCIPES DE PRATIQUES ÉQUITABLES DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Norme Nationale du Canada Intitulée Code type sur la protection des renseignements personnels (1996)

1. Responsabilité

Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci--dessous.

2. Détermination des fins de la collecte des renseignements

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant la collecte ou au moment de celle-ci.

3. Consentement

Toute personne doit être informée de toute collecte, utilisation ou divulgation de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

4. Limitation de la collecte

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

5. Limitation de l'utilisation, de la divulgation et de la conservation

Les renseignements personnels ne doivent pas être utilisés ou divulgués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

6. Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.

7. Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondent à leur degré de sensibilité.

8. Transparence

Un organisme doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

9. Accès aux renseignements personnels

Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

10. Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci--dessus en communiquant avec le ou les personnes responsables de les faire respecter au sein de l'organisation concernée.